



Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

July 25, 2017

**By Certified Mail
Return Receipt Requested**

Office of the Maine Attorney General
6 State House Station
Augusta, ME 04333

CONSUMER PROTECTION DIVISION
RECEIVED

AUG 01 2017

OFFICE OF ATTORNEY GENERAL

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client Woodside Hotels and Resorts ("Woodside"), to inform you of a potential security incident involving personal information for certain Woodside guests that may have affected eight Maine residents. Woodside will be notifying potentially affected individuals and outlining some steps they may take to help protect themselves.

Woodside was recently notified of a potential security incident by Sabre/SynXis, a company that operates an Internet-accessible reservation platform for the hotel industry. According to the information we have received from this vendor in a letter dated June 6, 2017, an unauthorized individual was able to gain access to Sabre's systems and view certain reservation information between August 10, 2016, and March 9, 2017. The information that was accessed may have included certain payment card information belonging to certain individuals who provided card information when making reservations at some Woodside properties.

Woodside takes the privacy of personal information seriously, and was deeply disappointed to learn that this vendor's incident could affect Woodside guests. Upon learning of the incident, Woodside promptly initiated an investigation into the incident and has communicated extensively with the vendor to learn more about what occurred. The vendor informed us that it engaged an outside forensic investigation firm to assist them in investigating and remediating the situation and has enhanced the security around its access credentials and the monitoring of system activity to further detect and prevent unauthorized access. In addition, the vendor has advised us that they notified law enforcement and the payment card brands of this incident.

Affected individuals are being notified via written letter. We have provided our list of individuals to Sabre's mailing vendor and are being told that the vendor will begin mailing these notices on or about August 9. A form copy of the notice being sent to the affected Maine residents is included for your reference.

Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

28543726.1

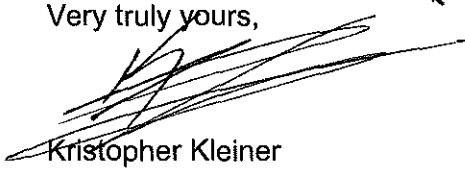
Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at nortonrosefulbright.com.

Office of the Maine Attorney General
July 25, 2017
Page 2

^NORTON ROSE FULBRIGHT

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Kristopher Kleiner', written over a horizontal line.

Kristopher Kleiner

KCK
Enclosure



[DATE]

[CUSTOMER NAME AND ADDRESS]

RE: [HOTEL]

Notice of Data Breach

Dear [CUSTOMER NAME]:

Woodside Hotels ("Woodside") was recently notified by its service provider, Sabre Hospitality Solutions ("Sabre"), of a third-party data security incident that may affect customer information associated with your hotel reservation(s) at the above-referenced hotel. The privacy and protection of our customers' information is a matter we take very seriously, and we are providing this notice as a precaution to let you know about the incident and tell you about some steps that you may take to protect yourself against potential misuse of your information.

What Happened

The Sabre SynXis Central Reservations system (CRS) facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. Following a forensic investigation, Sabre notified us, by letter dated June 6th, that an unauthorized party gained access to their systems and was able to view some reservation information for a subset of hotel reservations that Sabre processed on behalf of Woodside. The investigation determined that the unauthorized party was able to access Sabre's system between August 10th 2016 and March 9, 2017. Please note that no Woodside computer or network systems were affected in any way by this incident.

What Information Was Involved

The unauthorized party was able to access payment card information for certain hotel reservations, including cardholder names, card numbers, card expiration dates, and, potentially, card verification codes. The unauthorized party was also able, in some cases, to access certain information such as guest names, emails, phone numbers, addresses, and other information. Sensitive information such as Social Security, passport, or driver's license numbers were not accessed or affected by this incident. Sabre has informed us that, to date, the payment card brands have not identified any patterns of fraud related to this data breach.

What We Are Doing

According to the information that we received, Sabre engaged a leading cybersecurity firm to support its investigation and notified law enforcement and the payment card brands about this incident. Sabre also enhanced the security around access credentials and the monitoring of system activity to help prevent this type of incident from recurring in the future.

What You Can Do

You can review your credit or debit card account statements to determine if there are any discrepancies or

unusual activity listed. Remain vigilant and continue to monitor statements for unusual activity going forward. If you see something you do not recognize, immediately notify the card issuer as well as the proper law enforcement authorities. In instances of credit or debit card fraud, it is important to note that cardholders are not typically responsible for any fraudulent activity that is reported in a timely fashion.

Although Social security numbers and other sensitive personal information were not at risk in this incident, as a general practice you can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As an additional precaution, we are providing an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

We sincerely regret any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us toll-free at 888-721-6305 twenty-four hours per day, Monday through Friday. More information is also available at www.sabreconsumernotice.com.

Sincerely,

Gregory E. Alden
President and CEO

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Review of Accounts and Credit Reports: As a precaution you may regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the end of this guide.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft. There may be similar resources available at the state level, and you may contact your state department of revenue directly for more information.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request an initial fraud alert if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may request an extended fraud alert if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five

(5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity;
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
- (4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com)

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:

P.O. Box 740256, Atlanta, GA 30374
877-478-7625

Experian (www.experian.com)

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:

P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)

P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts and Security Freezes:

P.O. Box 2000, Chester, PA 19022
888-909-8872

Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

RECEIVED

JUL 31 2017

OFFICE OF ATTORNEY GENERAL

Notice of Data Breach

July 27, 2017

VIA FIRST CLASS MAIL

Janet T. Mills
6 State House Station
Augusta, ME 04333

Dear Attorney General Mills:

I am writing to inform you of an information security breach occurring at Cole Sport, including information provided by online shoppers using the Cole Sport online store located at www.colesport.com.

What Happened?

This incident relates to the unauthorized acquisition, by hackers, of certain information entered by customers on the Cole Sport online store checkout page. The hackers are believed to have accessed the information described below between March 27, 2017 to May 19, 2017. We initially became aware of the security incident on May 19, 2017 and we opened an internal investigation into the cause of the incident. However we did not understand the full scope of the incident (and the data affected) until July 14, 2017. We believe the incident has been contained and the unauthorized access terminated, and we believe that the relevant security vulnerability has been mitigated.

What Information Was Involved?

The information that may have been affected by this security incident includes information collected through our online ordering form. The information compromised varies by individual, but may include a customer's name, shipping and billing address, email address, payment card type, payment card number, expiration date, and verification number, and potentially, the user's [colesport.com](http://www.colesport.com) account password.

COLESPORT

What We Are Doing.

We continue to analyze the security incident, in partnership with our web development team, to learn more about the cause of the incident and prevent a similar issue from occurring in the future. Though the relevant security vulnerability is believed to have been remediated, we will continue to monitor the situation closely for any additional suspicious activity. Furthermore, we have applied important security updates to our systems and taken other proactive measures to help safeguard our services and protect customers' personal information. As an added precaution, we have arranged for identity theft protection at no cost to qualifying U.S. individuals whose payment card information was affected.

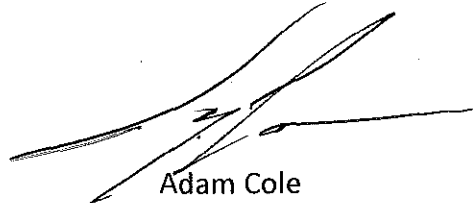
Notification and Number of Residents Affected

We believe that 1 resident of the state of Maine was affected by this breach. Where possible, this resident will be notified via first class U.S. mail, sent on or after the date of this letter above (as appropriate). A copy of the form letter mailed to the affected resident is attached to this letter.

Contact

If you have any questions you may contact counsel for Cole Sport directly at achambers@lewisbess.com or by phone at 303.228.2508.

Sincerely,



Adam Cole

Co-founder, Cole Sport

COLESPORT

Exhibit 1 – Template Notice to Consumers

[SEE ATTACHED]

Notice of Data Breach

July 27, 2017

[NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]

Dear [NAME],

Cole Sport takes the privacy and security of our customers' personal information seriously. Accordingly, we are writing to inform you of a security incident that may have affected certain personal information you provided to us when you recently shopped at our online store located at www.colesport.com.

Please see below under "What We Are Doing" for information on identity protection services we are making available to you at no charge. Additional resources are provided on the attached page.

What Happened?

This incident relates to the unauthorized acquisition, by hackers, of certain information entered by customers on the Cole Sport online store checkout page. The hackers are believed to have had access to the information described below between March 27, 2017 to May 19, 2017. We initially became aware of the security incident on May 19, 2017 and we opened an internal investigation into the cause of the incident. However we did not understand the full scope of the incident (and the data affected) until July 14, 2017. We believe the incident has been contained and the unauthorized access terminated and we believe that the relevant security vulnerability has been mitigated.

What Information Was Involved?

The information that may have been affected by this security incident includes information collected through our online ordering form. The information compromised varies by individual, but may include a customer's name, shipping and billing address, email address, payment card type, payment card number, expiration date, and verification number, and potentially, the user's [colesport.com](http://www.colesport.com) account password.

What We Are Doing.

We continue to investigate the security incident to learn more and prevent a similar issue from occurring in the future. We will continue to monitor the situation closely for any additional suspicious activity. Furthermore, we have applied important security updates to our systems and taken other proactive measures to help safeguard our services and protect your personal information.

As an added precaution, we have arranged to have Experian provide you with identity protection services for 12 months at no cost to you. The identity protection services will be available on the date of this notice and must be activated no later than October 31, 2017. For details on how to take advantage of these services, please see the instructions included on the attached page.

What You Can Do.

To help protect the security of your information, you can sign up for identity protection services as described above. In addition, please closely monitor your online and financial accounts, and be aware that criminals may attempt to use your payment card information to make purchases, send you targeted emails seeking to obtain other confidential information from you (i.e. phishing scams), or may otherwise try to use your personal information.

Always report any illegal activities to law enforcement or an appropriate government authority (see below for helpful resources). If you notice any unauthorized or fraudulent charges on your payment card or other suspicious financial activity, such as new credit applications, loans, or account openings, report it to the appropriate financial institution in addition to government authorities. Remember, Cole Sport will never ask for your username, password, or other sensitive personal information via email. If you receive an email from us or anyone else requesting this information, do not open any attachments and do not provide any personal information.

Because our investigation indicates that your colesport.com account password and email may have been affected, consider taking a moment to change your password on sites or for services where you may have used the same password as you did on our site. Information on creating strong passwords can be found on the Department of Homeland Security's website: <https://www.us-cert.gov/ncas/tips/ST04-002>.

For More Information.

If you have any questions regarding this notice or if you would like more information, please do not hesitate to contact Experian at 877-890-9332.

Most importantly, we sincerely regret any concern this security incident may cause. Our customers are the most important part of our business, and we value your trust and understanding.

Sincerely,

Adam Cole

Co-founder, Cole Sport

IMPORTANT INFORMATION

Experian Identity theft Protection Services

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one-year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **October 31, 2017** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/3bplusone**
- Provide your activation code

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **October 31, 2017**. Be prepared to provide engagement number **DB02680** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling

- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance:**² Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information:

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

Obtaining a Copy of your Credit Report

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report, or request information on how to place a fraud alert or security freeze on your credit file, by contacting any of the national credit bureaus below. Remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. The contact information for three major credit bureaus are as follows:

| | | |
|--|---|---|
| Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 www.equifax.com | Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com | TransUnion P.O. Box 1000 Chester, PA 19022 1-800-888-4213 www.transunion.com |
|--|---|---|

Contact Information for the Federal Trade Commission

In addition to the credit bureaus above, you may contact or visit the website of the Federal Trade Commission to learn more about how to protect yourself against identity theft, or how to place a fraud alert or security freeze on your credit file. The contact information for the FTC is as follows:

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

How to Place a Fraud Alert on Your Credit File

² Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

To protect yourself from the possibility of identity theft or other fraud, you may place a fraud alert on your credit file. The fraud alert helps to prevent someone else obtaining credit in your name. If you have a fraud alert on your credit file, creditors will contact you and verify your identity before they open any new accounts or change your existing accounts, but it should not affect your credit score or your ability to obtain new credit (although it may cause a delay in any applications or approvals). As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts, so you do not need to place alerts with more than one of the credit bureaus. To place a fraud alert, go to any of the following links and complete the requested steps:

<https://www.experian.com/fraud/center.html>

https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

<http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page>

How to Place a Security Freeze on Your Credit File

If you wish to take more extensive measures to prevent new credit being opened in your name, you may consider placing a security freeze on your credit file. You should only place a security freeze if you want to prevent most parties from obtaining your credit report and prevent all credit, loans and related services from being approved in your name without your consent. Please consider that this may also impact or delay your ability to obtain certain government services, rental housing, employment, cell phone plans, insurance, utilities, and other services.

You will need to apply for a security freeze separately with each of the credit bureaus. The requirements to obtain a security freeze vary depending on your state of residence, and you may be required to pay a fee, provide your name and social security number, copies of important identification records (including a list of addresses, copies of government issued IDs, and/or utility bills), provide an incident report if you are a victim of identity theft, or take other measures as described on the credit bureaus' websites. You may need to follow these steps for each individual (such as a spouse or dependent) who will request a security freeze. You can find more information regarding a security freeze at the following links, or by calling each of the credit bureaus at the numbers listed in this notification letter:

<https://www.freeze.equifax.com>

https://www.experian.com/consumer/security_freeze.html

<http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page>

Contact Information for State Government Agencies

You may also contact your state's attorney general or state department of revenue, as there may be more information available at the state level. Residents of California, Rhode Island, Maryland, and North Carolina are advised that they may contact their local law enforcement agencies using the following contact information:

| | | |
|--|---|--|
| Maryland Office of the Attorney General Identity Theft Unit 200 St. Paul Place, 16th Floor Baltimore, MD 21202 Phone: (410) 576-6491 Fax: (410) 576-6566; E-mail: idtheft@oag.state.md.us | California Attorney General's Office California Department of Justice Attn: Office of Privacy Protection P.O. Box 944255 Sacramento, CA 94244-2550 Tel: (916) 322-3360 Toll-free: (800) 952-5255 https://oag.ca.gov/idtheft | North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 Telephone: (919) 716-6400 Fax: (919) 716-6750 |
|--|---|--|

Maine



10402 Harwin Dr,
Houston TX, 77036
<https://www.directron.com>

July 28, 2017

Maine Office of the Attorney General
6 State House Station
Augusta, ME 04333

CONSUMER PROTECTION DIVISION
RECEIVED

JUL 31 2017

OFFICE OF ATTORNEY GENERAL

Re: NOTICE OF DATA BREACH
PLEASE READ CAREFULLY

Dear Sir or Madam:

Recently, Directron discovered that our information technology system was accessed by an unauthorized third party, and we regret to inform you that the personal information of 3 Maine residents may have been affected. We have notified our Maine customers of this potential access to their personal information.

What Happened?

On or about February 20, 2017 – April 24, 2017, transactions that our Maine customers initiated on the Directron website may have been compromised and information regarding such transactions may have been transmitted to an unauthorized third party. We discovered this unauthorized activity on or about May 9, 2017 and engaged a leading technology security firm to conduct a forensic audit of this matter. At this time, we are reasonably certain that the unauthorized activity stopped on or about May 10, 2017.

What Information Was Involved?

The information that may have been accessed included names, credit card information, CVV codes, billing and shipping addresses, email addresses, and your Directron website user name and password.

What We Are Doing

We take our obligation to safeguard our customers' personal information very seriously. As stated, we have engaged a technology security firm to assist us in determining the source and extent of the unauthorized access. If any additional significant developments occur, we will notify customers as soon as possible. Additionally, we have implemented measures to prevent a recurrence of this data breach and protect the privacy of our valued customers.

We also are working with the technology security firm to notify the major credit card companies. Therefore, our customers may receive a notice from their credit card company regarding this incident.

As required by law, we inform you that this breach did not require a law enforcement investigation and that this notice was not delayed due to law enforcement.

Maine

For More Information

Above all, we at Directron value our relationships with our customers and the trust that they place with us. We believe that we have successfully blocked any further access via the method used to compromise these transactions and will continue to review and strengthen our information technology systems and protocols in an ongoing effort to enhance security. If you have any questions or concerns regarding this matter, please call our information line anytime: (713) 933-1011 or contact us at facts@directron.us.

Attached is a sample copy of the notice being sent to our Maine resident customers. Attached to the notice is a Personal Information Security Guide that provides information for our customers on protecting their personal information. The Guide provides information on the right to request a police report, how to request a security freeze, and information that customers must provide when requesting a security freeze. We have also posted a copy of the Personal Information Security Guide, as well as fees required by credit reporting agencies in order to place a security freeze on your credit report, on our website at <https://www.directronfacts.com>.

Sincerely,

Julia Liu, President



10402 Harwin Dr,
Houston TX, 77036
<https://www.directron.com>

(DATE)

VIA EMAIL AND REGULAR FIRST CLASS MAIL

(Name)
(Address)
(City, State, Zip)

Re: NOTICE OF DATA BREACH
PLEASE READ CAREFULLY

Dear Customer:

Recently, Directron discovered that our information technology system was accessed by an unauthorized third party, and we regret to inform you that your personal information may have been affected.

What Happened?

On or about [transaction date(s)], a transaction you initiated on the Directron website may have been compromised and information regarding your transaction may have been transmitted to an unauthorized third party. We discovered this unauthorized activity on or about May 9, 2017 and engaged a leading technology security firm to conduct a forensic audit of this matter. At this time, we are reasonably certain that the unauthorized activity stopped on or about May 10, 2017.

What Information Was Involved?

The information that may have been accessed included names, credit card information, CVV codes, billing and shipping addresses, email addresses, and your Directron website user name and password.

What We Are Doing

We take our obligation to safeguard your personal information very seriously. As stated, we have engaged a technology security firm to assist us in determining the source and extent of the unauthorized access. If any additional significant developments occur, we will notify you as soon as possible. Additionally, we have implemented measures to prevent a recurrence of this data breach and protect the privacy of our valued customers.

We also are working with the technology security firm to notify the major credit card companies. Therefore, you may receive a notice from your credit card company regarding this incident.

As required by law, we inform you that this breach did not require a law enforcement investigation and that this notice was not delayed due to law enforcement.

Maine

What You Can Do

We deeply regret that this incident could affect you and are alerting you about this issue so you can take steps to protect yourself. The attached Personal Information Security Guide provides information on protecting your personal information. The Guide provides information on your right to request a police report, how to request a security freeze, and information that you must provide when requesting a security freeze. We have posted a copy of the Personal Information Security Guide, as well as fees required by credit reporting agencies in order to place a security freeze on your credit report, on our website at <https://www.directronfacts.com>.

For More Information

Above all, we at Directron value our relationships with our customers and the trust that you have placed with us. We believe that we have successfully blocked any further access via the method used to compromise these transactions and will continue to review and strengthen our information technology systems and protocols in an ongoing effort to enhance security. If you have any questions or concerns regarding this matter, please call our information line anytime: (713) 933-1011 or contact us at facts@directron.us.

Thank you for your continued support and for being a Directron customer.

Sincerely,

Julia Liu, President

PERSONAL INFORMATION SECURITY GUIDE

Review Your Account Statements and Order a Credit Report. In today's world, we all need to remain vigilant by regularly reviewing account statements and monitoring free credit reports. Under U.S. law, all citizens are entitled to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com.

Change Your Password. In the coming weeks, you will be prompted to change your password when you access Directron's website. We also recommend that you change your password for any other account in which you use the same or a similar password.

Credit Bureau Information

| | | |
|---|--|---|
| Equifax PO BOX 740241 Atlanta, GA 30374-0241 1-888-766-0008 equifax.com | Experian PO BOX 4500 ALLEN TX 75013 1-888-397-3742 experian.com | TransUnion PO BOX 2000 Chester, PA 19016 1-888-909-8872 transunion.com |
|---|--|---|

Right to Obtain a Police Report. You can also remain vigilant by contacting law enforcement in the event of actual or suspected identity theft. Call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be.

Fraud Alerts and Security Freezes. You can obtain additional information about fraud alerts and security freezes from the Federal Trade Commission (FTC) and the nationwide credit bureaus. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two bureaus, which then must also place fraud alerts in your file. In addition, you can visit the credit bureau links below to determine if and how you may place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your prior written authorization:

- Equifax security freeze: www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian security freeze: www.experian.com/consumer/security_freeze.html
- TransUnion security freeze: www.transunion.com/personal-credit/credit-disputes/credit-freezes.page
- Note that there can be varying fees associated with a security freeze request. Information on those fees is available at the links above, and on our website at <https://www.directronfacts.com>.

For Additional Information:

Visit the Federal Trade Commission website at:
www.ftc.gov, **call** 1-877-ID-THEFT, or **write to this address**:
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

MAINE SECURITY BREACH REPORTING FORM

Pursuant to the Notice of Risk to Personal Data Act

(Maine Revised Statutes 10 M.R.S.A. §§ 1346-1350-B)

Name and address of Entity that owns or maintains the computerized data that was subject to the breach:

Steel Technology LLC dba Hydro Flask

Street Address: 525 NW York Drive

City: Bend State: OR Zip Code: 97703

Submitted by: Leticia Limon Title: Assistant General Counsel Dated: 7/28/17

Firm Name (if other than entity): Helen of Troy, L.P.

Telephone: 915-225-5864 Email: llimon@hotus.com

Relationship to Entity whose information was compromised: Representative of Parent Company

Type of Organization (please select one): ☐ Governmental Entity in Maine; ☐ Other Governmental Entity;

☐ Educational; ☐ Health Care; ☐ Financial Services; * ☒ Other Commercial; ☐ Not-for-Profit

Number of Persons Affected:

Total (including Maine residents): 40,942 Maine Residents: 132

If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified? ☐ Yes; ☐ No.

Dates: Breach Occurred: Approx. 2/10/17 Breach Discovered: 05/02/17 Consumer Notification: 7/25/17

Description of Breach (please select all that apply):

☐ Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);

☐ Internal system breach; ☐ Insider wrongdoing; ☒ External system breach (e.g., hacking); ☐ Inadvertent disclosure;

☐ Other (specify): _____

Information Acquired: Name or other personal identifier in combination with (please select all that apply):

☐ Social Security Number

☐ Driver's license number or non-driver identification card number

☒ Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons – ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED MAINE RESIDENTS:

☒ Written; ☐ Electronic; ☐ Telephone; ☐ Substitute notice.

List dates of any previous (within 12 months) breach notifications: 11/2/16

Identity Theft Protection Service Offered: ☒ Yes; ☐ No.

Duration: 1 Year Provider: Experian

Brief Description of Service: Credit Monitoring, Fraud Consultation and Identity Theft Restoration

*If reporting to Department of Professional and Financial Regulation, this form is not required. 10 M.R.S.A. § 1348(5)

PLEASE COMPLETE AND SUBMIT THIS FORM TO

Fax or E-mail this form to:

Maine State Attorney General's Office
SECURITY BREACH NOTIFICATION
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, Maine 04330
Fax: 207-624-7730
E-mail: breach.security@maine.gov



<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

NOTICE OF DATA BREACH

Dear <<MemberFirstName>> <<MemberLastName>>,

Steel Technology, LLC, doing business as Hydro Flask ("Hydro Flask") is writing to provide you with information about a recent system disruption Hydro Flask experienced.

WHAT HAPPENED

On or about May 2, 2017, Hydro Flask learned that the security of personal information Hydro Flask received about you during your visit to our e-commerce website (<http://www.hydroflask.com/>) may have been compromised.

WHAT ARE WE DOING

Upon becoming aware of the system disruption, Hydro Flask immediately took actions to secure its security systems by engaging recognized security consultants to investigate the nature of the disruption, conducting system scans, resetting access credentials, and building a new server.

We have also secured the services of Kroll to provide you one year of identity monitoring at no cost to you. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

*You have until **October 26, 2017** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-855-366-0139. Additional information describing your services is included with this letter.

WHAT INFORMATION WAS INVOLVED

Although Hydro Flask is still investigating the scope of the disruption, Hydro Flask believes that an intruder may have had unauthorized access to customer order pages on our website that may have contained your name, billing and shipping address, email address, and credit card information.

WHAT YOU CAN DO

For your security, Hydro Flask encourages you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. Neither Hydro Flask nor anyone acting on its behalf will contact you in any way, including by email, to ask for your credit card number, Social Security number or other personal information. If you are asked for this information, you can be confident Hydro Flask is not the entity asking.

OTHER IMPORTANT INFORMATION

To protect against possible identity theft or other financial loss, Hydro Flask encourages you to remain vigilant, review your financial account statements and monitor your credit reports. Hydro Flask is also providing the following information for those who wish to consider it:

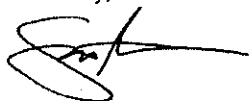
- You may wish to visit the website of the U.S. Federal Trade Commission at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.
- **Maryland Residents.** You can reach the Maryland Attorney General at 888-743-0023 (toll free in Maryland) or Office of the Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202
- **North Carolina Residents.** You can reach the North Carolina Attorney General at 919-716-6400 or Office of the Attorney General, 9001 Mail Service Center, Raleigh, North Carolina 27699-9001
- **Rhode Island Residents.** You can reach the Rhode Island Attorney General at 401-274-4400 or Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903
- **Iowa, Massachusetts, Oregon, and Rhode Island Residents.** You have the right to obtain any police report filed related to this intrusion, and to file a police report and obtain a copy of it if you are the victim of identity theft.
- If you are a U.S. resident, under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.
- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide your: (1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the consumer reporting agencies listed below.
 - Experian: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
 - Equifax: 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348
 - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

Please note that fees may be required to be paid to the consumer reporting agencies listed above.

FOR MORE INFORMATION

If you have questions, please call 1-855-366-0139, Monday through Friday from 6:00 a.m. to 3:00 p.m. Pacific Time. Please have your membership number ready. We apologize for any inconvenience this may cause you.

Sincerely,



Scott Allan
General Manager
Hydro Flask



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

CONSUMER PROTECTION DIVISION
RECEIVED

AUG 07 2017

OFFICE OF ATTORNEY GENERAL

RECEIVED

AUG 04 2017

OFFICE OF ATTORNEY GENERAL

July 31, 2017

**FIRST-CLASS MAIL
VIA E-MAIL**

data breach

Attorney General Janet T. Mills
Maine State Attorney General's Office
SECURITY BREACH NOTIFICATION
Consumer Protection Division
111 Sewall Street, 6th Floor
August, Maine 04330
breach.security@maine.gov

Re: Voluntary ~~Security Incident Notice Provided for Paris Las Vegas Operating Company,~~
LLC d/b/a Paris Las Vegas

Dear Attorney General Janet T. Mills,

This firm represents Paris Las Vegas Operating Company, LLC d/b/a Paris Las Vegas ("Paris Las Vegas") with respect to an incident involving the potential exposure of certain personal information on a reservation system owned and operated by Sabre Hospitality Solutions ("Sabre").

Nature of the Incident.

Sabre's SynXis Central Reservations (SynXis) system allows travel agents and others to search for and reserve rooms at thousands of hotels, including at Paris Las Vegas. Paris Las Vegas recently learned that the Sabre SynXis system experienced a data security incident. According to Sabre's investigation, some hotel reservations processed through the SynXis system from August 10, 2016 to March 9, 2017 may have been accessed without authorization. An unauthorized party obtained access to credentials on Sabre's system, which could have permitted unauthorized access to reservation information on Sabre's system, including guests' names and credit card numbers, and also may have included card expiration dates, security codes, and mailing addresses.

The property management systems for Paris Las Vegas were not involved. In addition, Paris Las Vegas never receives credit card information from Sabre for reservation transactions. Instead, Paris Las Vegas processes reservations from Sabre using tokens. As a result, Paris Las Vegas does not receive the guest card holder name, card number, expiration date, or security code that may have been given to Sabre by the guest or the guest's travel agent.

On June 6, 2017, Sabre gave Paris Las Vegas limited information to assist in identifying potentially affected guests. Based on this limited information, Paris Las Vegas was able to identify some guests whose reservation information may have been involved in Sabre's data security incident.

Because Paris Las Vegas values its guests' privacy and security, Paris Las Vegas is voluntarily notifying affected guests concerning Sabre's data security incident. Paris Las Vegas also is providing its guests with two free years of credit monitoring and identity protection services through Equifax.[®] We have attached a sample of the notification letters that are being provided to identified guests.

Number of Maine Residents Affected.

The data set at issue included one Maine resident. A notification letter is being sent to this resident via regular mail on July 31, 2017.

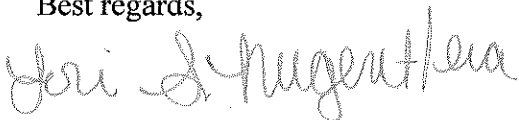
Steps Taken and Plans Relating to the Incident.

Paris Las Vegas is providing notification to its guests out of an abundance of caution and encouraging its guests to closely monitor their credit card statements and report any unusual activity. Paris Las Vegas also engaged Epiq Solutions to provide mailing and call centering services, as well as two years of credit monitoring and identity protection services through Equifax[®] at no cost to the guests.

Contact Information.

Should you have any questions or if additional information is needed, please do not hesitate to contact me at nugentl@gtlaw.com or 214-665-3630.

Best regards,



Lori S. Nugent
Shareholder

Enclosure

MAINE SECURITY BREACH REPORTING FORM

Pursuant to the Notice of Risk to Personal Data Act

(Maine Revised Statutes 10 M.R.S.A. §§ 1346-1350-B)

Name and address of Entity that owns or maintains the computerized data that was subject to the breach:

Paris Las Vegas Operating Company, LLC d/b/a Paris Las Vegas

Street Address: 3655 Las Vegas Boulevard South

City: Las Vegas State: NV Zip Code: 89109

Submitted by: Lori S. Nugent Title: Shareholder; Data Security, Privacy & Crisis Management
Dated: 7/31/2017

Firm Name (if other than entity): Greenberg Traurig LLP

Telephone: 214-665-3630 Email: nugentl@gtlaw.com

Relationship to Entity whose information was compromised: Outside Counsel

Type of Organization (please select one): ☐ Governmental Entity in Maine; ☐ Other Governmental Entity;
☐ Educational; ☐ Health Care; ☐ Financial Services; * ☒ Other Commercial; ☐ Not-for-Profit

Number of Persons Affected:

Total (including Maine residents): 88 Maine Residents: 1

If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified? ☒ Yes; ☐ No

Dates: Breach Occurred: 8/10/2016 Breach Discovered: 6/6/2017 Consumer Notification: 7/31/2017

Description of Breach (please select all that apply):

☐ Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
☐ Internal system breach; ☐ Insider wrongdoing; ☐ External system breach (e.g., hacking); ☐ Inadvertent disclosure;
☒ Other (specify): Third party vendor experienced external system breach.

Information Acquired: Name or other personal identifier in combination with (please select all that apply):

☐ Social Security Number
☐ Driver's license number or non-driver identification card number
☒ Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons – ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED MAINE RESIDENTS:

☒ Written; ☐ Electronic; ☐ Telephone; ☐ Substitute notice.

List dates of any previous (within 12 months) breach notifications:

Identity Theft Protection Service Offered: ☒ Yes; ☐ No.

Duration: 2 Years Provider: Equifax

Brief Description of Service: Identity Protection Services & Credit Monitoring

*If reporting to Department of Professional and Financial Regulation, this form is not required. 10
M.R.S.A. § 1348(5)

PLEASE COMPLETE AND SUBMIT THIS FORM TO

Fax or E-mail this form to:

Maine State Attorney General's Office
SECURITY BREACH NOTIFICATION
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, Maine 04330
Fax: 207-624-7730
E-mail: breach.security@maine.gov

July 31, 2017

«First_Name» «Last_Name»
«Street_Address»
«Address_2»
«City», «State» «Zip»

Dear «First_Name» «Last_Name»

We recently learned that a reservation system owned and operated by Sabre Hospitality Solutions (Sabre) experienced a data security incident. Our systems at Paris Las Vegas were not involved, but Sabre has informed us that information on its system about your reservation at Paris Las Vegas may have been accessed without authorization.

We value the privacy and security of our guests' information, and we are sorry for any inconvenience that Sabre's incident may cause.

What Happened?

Sabre's SynXis Central Reservations (SynXis) system allows travel agents and others to search for and reserve rooms on behalf of their clients at thousands of hotels, including at our property. According to Sabre's investigation, some hotel reservations processed through the SynXis system from August 10, 2016 to March 9, 2017 may have been accessed without authorization. An unauthorized party obtained access to credentials on Sabre's system, which could have permitted unauthorized access to your reservation information.

What Information Was Involved?

Sabre's investigation indicated that certain reservation information may have been accessed without authorization. The information included guests' names and credit card numbers, and also may have included card expiration dates, security codes, and mailing addresses.

On June 6, 2017, Sabre gave us limited information to assist us in identifying guests who may have been affected by this incident. Based on this limited information, we were able to determine that your reservation information may have been involved in Sabre's data security incident. Sabre did not, however, provide us the card holder name or address for the credit card used for the reservation, so we are unable to determine if the credit card used for your reservation belongs to you or another person.

Our hotel never receives credit card information from Sabre for any reservation transactions. To process credit card transactions for reservations made using the Sabre system, credit card information is transmitted from the Sabre system to our third party credit card payment processor.

What Sabre is Doing

Sabre retained a leading cybersecurity firm to investigate the incident. Additionally, Sabre notified law enforcement and the credit card companies about this incident so that they can coordinate monitoring of the credit cards at issue. Sabre has also indicated that it has secured its system.

What We are Doing

Because we value you as our guest, we want to make sure you are aware of this incident. To ease any concern you may have, at no cost to you, we are providing you with two years of credit monitoring and identity protection services through Equifax® as described below.

What Can Affected Individuals Do?

We are alerting you to this incident so that you can take steps to protect your information. It is a good practice to carefully review your credit card statements and quickly report anything unusual to your financial institution or credit card company. There are rules that limit a credit card company's reimbursement for fraudulent credit card charges when a problem is not reported quickly.

As a precautionary measure to help better protect your credit file from potential misuse, we have partnered with Equifax[®] to provide its Credit Watch[™] Silver credit monitoring and identity theft protection product for two years at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code).

If you choose to take advantage of this product, it will provide you with a notification of key changes to your Equifax credit file, up to \$25,000 Identity Theft Insurance¹ Coverage, automatic fraud alerts,² access to your Equifax credit report and Identity Restoration. If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

Even if you decide not to take advantage of the subscription offer, you may still receive Equifax Identity Restoration in the event that you become victim of identity theft by calling 877-368-4940, 9:00 a.m. to 8:00 p.m. Eastern, Monday through Friday, before August 1, 2019.

You must complete the enrollment process for Equifax Credit Watch[™] Silver by November 1, 2017. We urge you to consider enrolling in this product, at our expense, and reviewing the attached materials enclosed with this letter.

For More Information

If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us at 1-800-572-9349. We are available Monday through Friday from 9:00 a.m. to 9:00 p.m. EST.

Sincerely,

Paris Las Vegas Operating Company, LLC d/b/a Paris Las Vegas
3655 Las Vegas Boulevard, South
Las Vegas, NV 89019



Activation Code: «Redemption_Code»

About the Equifax Credit Watch™ Silver identity theft protection product

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available
- One copy of your Equifax Credit Report™
- \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality *
- Identity Restoration If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

How to Enroll: You can sign up online

To sign up online for online delivery go to
www.myservices.equifax.com/silver

1. Welcome Page: Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

State Notification Requirements

All States.

You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
1-800-680-7289
Chester, PA 19016
www.transunion.com

For residents of Massachusetts and Rhode Island.

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts, Rhode Island, and West Virginia.

You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

For residents of Iowa.

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon.

State laws advise you to report any suspected identity theft to law enforcement, as well as the Attorney General and Federal Trade Commission.

For residents of Illinois, Maryland, Rhode Island and North Carolina.

You can obtain information from the Federal Trade Commission, and for residents of Maryland and North Carolina, from your respective state Office of the Attorney General, about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection Unit
(401) 274-4400
<http://www.riag.ri.gov>

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

July 31, 2017

Jena Valdetero
Direct: (312) 602-5056
jena.valdetero@bryancave.com**VIA US MAIL & EMAIL**

Maine Attorney General's Office
SECURITY BREACH NOTIFICATION
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, Maine 04330
E-mail: breach.security@maine.gov

CONSUMER PROTECTION DIVISION**RECEIVED****AUG 04 2017****OFFICE OF ATTORNEY GENERAL**

Re: Voluntary Data Security Breach Notification

To Whom It May Concern:

A client of Bryan Cave LLP, intends to notify thirty-three (33) residents of Maine of a criminal cyber-attack involving a third party business partner, Sabre Hospitality Solutions ("Sabre"). Sabre facilitates and processes certain reservations for the hotels identified in the attached exhibit which are operated by our client. We are providing this letter as a courtesy although, based upon the facts of the incident, notification may not be required under 10 M.R.S. 1348.

On June 6th, Sabre made our client aware of an attack which allowed an unauthorized third party to access Sabre's systems using authorized log-in credentials between August 10, 2016 and March 9, 2017. Sabre reports that it enlisted a leading forensics firm to help in its investigation. Sabre has stated, but our client has not been able to independently confirm, that:

- Sabre stopped the intrusion,
- Sabre identified all reservations that were potentially accessed,
- Sabre excluded the unauthorized individual from its systems,
- The unauthorized party was able to access payment card information for hotel reservation(s), including credit or debit cardholder name; card number; card expiration date; and, in some instances, card security code; in certain cases, the guest's name, email, phone number, address, number of adults and children staying at the hotel, and dates of reservation at one or more of the referenced hotels were also unlawfully accessed, and
- Sabre notified the payment card brands of this incident.

Our client is notifying potentially affected customers in early August, 2017 via U.S. mail through a service provider retained by Sabre. An example of the customer message is attached. If you would

like any additional information concerning the above event, please feel free to contact me at your convenience.

Sincerely,

/s/ Jena Valdetero

Jena Valdetero

Attachments

EXHIBIT

Big Meadows Lodge

Cedar Grove

Explorer Cabins at Yellowstone

Gideon Putnam Hotel

Grant Grove Village

Gray Wolf Inn & Suites

Honey Creek Resort State Park

Kalaloch Lodge

Lewis Mountain Cabins

Peaks of Otter Lodge

Pine Lodge

Rocky Mountain Park Inn

Sea Crest Beach Hotel

Skyland Resort

Tenaya Lodge

The Lodge at Geneva

Trailer Village RV Park

Wheeling Island Hotel

Wuksachi Lodge

Yavapai Lodge

Yellowstone Park Hotel

[DATE]

[CUSTOMER NAME AND ADDRESS]

NOTICE OF DATA BREACH

Dear Valued Guest:

Sabre Hospitality Solutions, which facilitates and processes the booking of reservations for many hotels including [INSERT NAME OF HOTEL], recently, indicated that they experienced a data breach.

While the breach only impacted Sabre and did not compromise the computer networks and guest data at your hotel, we are providing this notification to you as Sabre has indicated that your information may have been impacted. We have enclosed a letter from Sabre that explains the incident, as well as some general information about identity theft.

What Happened?

Sabre indicated that confidential payment card and other guest reservation data from August 10, 2016 to March 9, 2017, that was held in their reservation system was unlawfully accessed by an unauthorized person. They have further indicated that your booking information was on Sabre's server during that period of time, and, as a result, your information may have been at risk. Sabre has not indicated how many individuals were impacted by the breach overall, or how many individuals were impacted from your state.

What Information Was Involved?

Sabre has indicated that the unauthorized party was able to access payment card information, including such information as credit or debit cardholder name, card number, card expiration date and card security code. In addition, in certain cases, the guest's name, email, phone number, address, number of adults and children staying at the hotel, and dates of reservation at the hotel were also unlawfully accessed.

What We Are Doing

Sabre has informed us that they notified law enforcement and the payment card brands about the security breach of its network and of the confidential data that was accessed. Sabre also retained a

payment card industry forensic investigator to investigate this incident. Sabre has established a website with information about the breach (www.sabreconsumerhelp.com).

We asked that Sabre provide you with the attached notice to give you more information about the breach. Although we are not able to independently verify the information therein, we are continuing to discuss with Sabre how the incident happened and to obtain assurances from them of their ongoing security and how they will handle and investigate security incidents like this in the future.

What You Can Do

Under the circumstances, we strongly recommend that you regularly monitor your credit or debit card account statements for any unauthorized activity. If you discover any suspicious or unusual activity on your payment card account, immediately notify your account institution. In addition, be vigilant about any emails that you may receive that claim to be from the hotel or Sabre, particularly any emails that ask you to provide personal information or click on links.

For More Information

Additional information about how to protect yourself, including state-specific information, is enclosed in the attached sheet titled "Additional Information and Resources about Identity Theft." If you have any questions regarding the Sabre data breach or if you desire further information or assistance, Sabre has set up a toll-free hotline which can be reached at 888-721-6305.

We sincerely apologize if you experience any inconvenience because of the Sabre data breach. The privacy and protection of customer information is of the utmost importance to us, and we are committed to working with Sabre to make sure that they continue to take appropriate steps to protect guest data.



June XX, 2017

Dear [Insert Brand] Customers:

Sabre is a leading technology provider to the global travel industry, and counts [Insert Brand] as one of our most important customers of our Sabre Hospitality Solutions (SHS) division.

SHS had a cybersecurity incident that affects you. We wanted to offer an explanation.

SHS provides reservations technology to a number of hotels. SHS had an incident in which an unauthorized party was able to obtain the credentials to an account within the SHS central reservations system and then view a subset of the hotel reservations. This was not an internal technology platform at a hotel that you stayed at, and the unauthorized use was contained to one system managed by SHS. As part of this incident, payment card information that may have been transmitted as part of the reservation booking process may have been viewed by this unauthorized user.

Sabre engaged premier cybersecurity experts to support our investigation and took successful measures to ensure this unauthorized access was stopped and is no longer possible. The investigation did not uncover evidence that the unauthorized party removed any information from the system, but it is a possibility. We have also notified law enforcement and the payment card brands.

The unauthorized party was able to access information for certain hotel reservations, including cardholder name; payment card number; card expiration date; and, for a subset of reservations, card security code (if it was provided). Social Security, passport, driver's license or other government identification numbers were not accessed.

On behalf of the Sabre team, we wish to express our sincere regret for this incident and assure you that we have taken measures to further strengthen our already-robust cybersecurity program. As a leading technology provider to the travel industry, Sabre is committed to a global, holistic security program focused on protecting its systems, their customers and consumers. As cyber threats have escalated, so too has Sabre's investment in state of the art security technology and highly qualified personnel to reassure its travel industry customers and the traveling public that Sabre addresses security with the utmost care and expertise.

Yours truly,

SABRE HOSPITALITY SOLUTIONS

ADDITIONAL INFORMATION AND RESOURCES

ABOUT IDENTITY THEFT

You may find the following general information and resources helpful concerning identity theft.

Federal Trade Commission

You may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

(877)-IDTHEFT (438-4338)
<https://www.identitytheft.gov/>

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

No Social Security Numbers or driver's license numbers were exposed in this incident, and, as a result, we have no reason to believe that you may be at risk of new account identity theft. As a general matter, it is advisable to regularly monitor your credit reports to see if any new accounts have been opened under your name. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the credit reporting agency delete that information from your credit report file.

You may contact the nationwide credit reporting agencies at:

| | | |
|--|--|--|
| Equifax | Experian | TransUnion |
| P.O. Box 105788 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19016 |
| (800) 525-6285 | (888) 397-3742 | (800) 680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of

your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Fraud Alert or Security Freeze on Your Credit Report File

Although no Social Security Numbers or driver's license numbers were exposed in this incident, and, as a result, we have no reason to believe that you may be at risk of new account identity theft, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

STATE SPECIFIC INFORMATION

IF YOU ARE AN IOWA RESIDENT:

You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa

Hoover State Office Building

1305 E. Walnut Street

Des Moines, IA 50319

(515) 281-5164

www.iowaattorneygeneral.gov

IF YOU ARE A MARYLAND RESIDENT:

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office.

This office can be reached at:

Office of the Attorney General

Consumer Protection Division

200 St. Paul Place

Baltimore, MD 21202

(888) 743-0023

www.marylandattorneygeneral.gov

IF YOU ARE A MASSACHUSETTS RESIDENT:

Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies, Equifax, Experian, and TransUnion, by regular, certified, or overnight mail or online at the addresses in the enclosed letter.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express, or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

IF YOU ARE A NEW MEXICO RESIDENT:

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. the unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. proper identification to verify your identity;
3. information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
4. payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies using the contact information provided in the enclosed letter.

IF YOU ARE A NORTH CAROLINA RESIDENT:

You may obtain information about preventing identity theft from the North Carolina Attorney General's

Office or the Federal Trade Commission. This office can be reached at:

North Carolina Department of Justice

Attorney General's Office

9001 Mail Service Center

Raleigh, NC 27699-9001

(877) 566-7226

<http://www.ncdoj.gov>

IF YOU ARE AN OREGON RESIDENT:

You may contact law enforcement, including the Oregon Attorney General's Office or the Federal Trade Commission to report suspected incidents of identity theft. .

This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
<http://www.doj.state.or.us/>

IF YOU ARE A RHODE ISLAND RESIDENT:

You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at:

RI Office of the Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
(401) 274-4400

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

Unless you are sixty-five (65) years of age or older, or you are a victim of identity theft with an incident report or complaint from a law enforcement agency, a consumer reporting agency has the right to charge you up to ten dollars (\$10.00) to place a freeze on your credit report; up to ten dollars (\$10.00) to temporarily lift a freeze on your credit report, depending on the circumstances; and up to ten dollars (\$10.00) to remove a freeze from your credit report. If you are sixty-five (65) years of age or older or are a victim of identity theft with a valid incident report or complaint, you may not be charged a fee by a consumer reporting agency for placing, temporarily lifting, or removing a freeze.

To place a security freeze on your credit report, you must apply online or send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided in the enclosed letter.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment. Do not send cash through the mail.



55 East Monroe Street
37th Floor
Chicago, IL 60603

312 346 7500 main
312 580 2201 fax
thompsoncoburn.com

Melissa K. Ventrone
312 580 2219 direct
mventrone@thompsoncoburn.com

July 31, 2017

CONSUMER PROTECTION DIVISION
RECEIVED

AUG 07 2017

Attorney General Janet T. Mills
Office of the Attorney General
6 State House Station
Augusta, ME 04333

OFFICE OF ATTORNEY GENERAL

Dear Attorney General Mills:

We represent Northwest Rheumatology ("NW Rheumatology") with respect to a recent security incident involving the potential exposure of certain protected health information described in more detail below. NW Rheumatology is a rheumatology clinic in Tucson, Arizona.

1. Nature of security incident.

On April 10, 2017, Northwest Rheumatology experienced a ransomware incident which left a limited portion of its computer system encrypted and inaccessible. NW Rheumatology immediately contacted its computer security vendor who investigated the matter and informed NW Rheumatology that no protected health information was accessed or acquired during the incident. Based on this report, NW Rheumatology believed that the attack on its systems was limited and that patient information was not affected.

However, on June 18, 2017, NW Rheumatology discovered additional evidence of unauthorized access to its systems from the ransomware attack. NW Rheumatology immediately hired an independent computer forensic firm to conduct an in-depth investigation. On July 6, 2017, the forensic team confirmed that an unauthorized individual had gained access to NW Rheumatology systems but was unable to determine whether any protected health information had actually been accessed.

2. Number of Maine residents affected.

NW Rheumatology has identified records for two (2) Maine residents impacted as a result of this incident. A notification letter was mailed to the individuals on July 31, 2017 via regular mail. Enclosed please find a copy of the notification letter.

3. Steps you have taken or plan to take relating to the incident.

NW Rheumatology is taking steps to prevent this sort of incident from occurring in the future. NW Rheumatology has reviewed and updated its internal password policies with new, more

July 31, 2017
Page 2

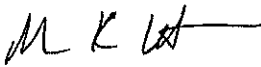
rigorous requirements, and has implemented new security measures to further secure the information in its systems from unauthorized access..

4. Contact information.

NW Rheumatology remains dedicated to protecting the sensitive information in its systems. If you have any questions or need additional information, please do not hesitate to contact me at MVentrone@ThompsonCoburn.com or (312) 580-2219.

Very truly yours,

Thompson Coburn LLP

A handwritten signature in black ink, appearing to read "M K Ventrone", with a horizontal line extending from the end.

Melissa K. Ventrone

Enclosures

NORTHWEST RHEUMATOLOGY

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name1>>

<<Address1>>

<<Address2>>

<<City>>, <<ST>> <<ZIP>>

<<Country>>

<<Date>>

Notice of Data Security Incident

Dear <<Name1>>:

We are writing to inform you about a data security incident experienced by Northwest Rheumatology ("NW Rheumatology") that may have exposed your personal information, including your name and Social Security number. We value and respect the privacy of your information, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

1. What happened and what information was involved?

On April 10, 2017, NW Rheumatology experienced a ransomware attack that encrypted a limited amount of information on our systems. We immediately had our computer security vendor conduct an investigation. The vendor informed us that no personal health data was accessed or acquired by an unauthorized individual. Based on this report, we believed our systems, and the information stored in our systems, were secure.

On June 18, 2017, while finalizing our internal recovery efforts related to the incident, our computer security vendor informed us that they had discovered additional evidence of unauthorized access to our systems. We immediately hired an independent computer forensic firm to conduct an in-depth investigation. On July 6, 2017, our forensic investigator informed us that an unauthorized individual had gained access to our systems, but they could not tell us whether any personal health information was accessed as a result of this access.

Because we are unable to determine with certainty that your information was not accessed, we thought it important to inform you of this incident and provide you with resources to help you protect your information. From our review, it appears that your name, address, Social Security number, health insurance information, diagnosis information, medical records, diagnoses, and demographic data may have been stored on our systems.

2. What we are doing and what you can do.

Securing your personal information is important to us. As a precautionary measure to help better protect your credit file from potential misuse, we have partnered with Equifax[®] to provide its Credit Watch[™] Silver credit monitoring and identity theft protection product for one year at no charge to you. A description of this product is provided below, along with instructions about how to enroll (including your personal activation code).

If you choose to take advantage of this product, it will provide you with a notification of key changes to your Equifax credit file, up to \$25,000 Identity Theft Insurance¹ Coverage, automatic fraud alerts², access to your Equifax credit report and Identity Restoration. If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

Even if you decide not to take advantage of the subscription offer, you may still receive Equifax Identity Restoration in the event that you become victim of identity theft by calling 877-368-4940, 9:00a.m. to 8:00p.m. Eastern, Monday through Friday, before July 31, 2018.

You must complete the enrollment process for Equifax Credit Watch[™] Silver by October 31, 2017. We urge you to consider enrolling in this product, at our expense, and reviewing the Additional Resources enclosed with this letter.



Activation Code: <<INSERT Credit Monitoring Code>>

About the Equifax Credit Watch™ Silver identity theft protection product

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available
- One copy of your Equifax Credit Report™
- \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality *
- Identity Restoration If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

How to Enroll: You can sign up online

To sign up online for **online delivery** go to www.myservices.equifax.com/silver

1. Welcome Page: Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf

Please review the enclosed additional information section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We want to assure you that we are taking steps to prevent this sort of incident from occurring in the future. NW Rheumatology has reviewed and updated its internal password policies with new, more rigorous requirements, and we have rolled out new security measures to further secure the information in our systems from unauthorized access.

3. For more information.

If you have questions, please call 800-342-9326 Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. Please have your membership number ready. Your trust is a top priority for us, and we deeply regret any inconvenience or concern this matter may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ulker Tok', with a stylized flourish at the end.

Dr. Ulker Tok
NW Rheumatology

U.S. State Notification Requirements

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax

P.O. Box 105139
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General

Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the Attorney General

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below:

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://www.experian.com/freeze>

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.

AUG 01 2017



OFFICE OF ATTORNEY GENERAL

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

NOTICE OF DATA BREACH

Dear <<MemberFirstName>> <<MemberLastName>>,

Steel Technology, LLC, doing business as Hydro Flask ("Hydro Flask") is writing to provide you with information about a recent system disruption Hydro Flask experienced.

WHAT HAPPENED

On or about May 2, 2017, Hydro Flask learned that the security of personal information Hydro Flask received about you during your visit to our e-commerce website (<http://www.hydroflask.com/>) may have been compromised.

WHAT ARE WE DOING

Upon becoming aware of the system disruption, Hydro Flask immediately took actions to secure its security systems by engaging recognized security consultants to investigate the nature of the disruption, conducting system scans, resetting access credentials, and building a new server.

We have also secured the services of Kroll to provide you one year of identity monitoring at no cost to you. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

You have until October 26, 2017 to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-855-366-0139. Additional information describing your services is included with this letter.

WHAT INFORMATION WAS INVOLVED

Although Hydro Flask is still investigating the scope of the disruption, Hydro Flask believes that an intruder may have had unauthorized access to customer order pages on our website that may have contained your name, billing and shipping address, email address, and credit card information.

WHAT YOU CAN DO

For your security, Hydro Flask encourages you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. Neither Hydro Flask nor anyone acting on its behalf will contact you in any way, including by email, to ask for your credit card number, Social Security number or other personal information. If you are asked for this information, you can be confident Hydro Flask is not the entity asking.

OTHER IMPORTANT INFORMATION

To protect against possible identity theft or other financial loss, Hydro Flask encourages you to remain vigilant, review your financial account statements and monitor your credit reports. Hydro Flask is also providing the following information for those who wish to consider it:


- You may wish to visit the website of the U.S. Federal Trade Commission at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.
- **Maryland Residents.** You can reach the Maryland Attorney General at 888-743-0023 (toll free in Maryland) or Office of the Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202
- **North Carolina Residents.** You can reach the North Carolina Attorney General at 919-716-6400 or Office of the Attorney General, 9001 Mail Service Center, Raleigh, North Carolina 27699-9001
- **Rhode Island Residents.** You can reach the Rhode Island Attorney General at 401-274-4400 or Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903
- **Iowa, Massachusetts, Oregon, and Rhode Island Residents.** You have the right to obtain any police report filed related to this intrusion, and to file a police report and obtain a copy of it if you are the victim of identity theft.
- If you are a U.S. resident, under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.
- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide your: (1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the consumer reporting agencies listed below.
 - Experian: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
 - Equifax: 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348
 - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

Please note that fees may be required to be paid to the consumer reporting agencies listed above.

FOR MORE INFORMATION

If you have questions, please call 1-855-366-0139, Monday through Friday from 6:00 a.m. to 3:00 p.m. Pacific Time. Please have your membership number ready. We apologize for any inconvenience this may cause you.

Sincerely,



Scott Allan
General Manager
Hydro Flask



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.